IN THE CLAIMS

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with <u>underlining</u> and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims in accordance with the following:

Please CANCEL the claims according to the following:

1.   (CURRENTLY AMENDED) A system for conducting an agreement between two parties relying on a trusted third party comprising:

<u>a mobile device as</u> a first party <u>independently of the second and third party</u> generating a first view of the agreement <u>secured based upon both a first mobile device parameter stored in the mobile device and a second mobile device parameter input to the mobile device</u> and transmitting the first view of the agreement to the ~~third~~<u>second</u> party;

a second party independently <u>of the first and third party</u> generating a second <u>secured</u> view of the agreement and transmitting the second <u>secured</u> view of the agreement to the third party;

~~a~~<u>an open and non-secure</u> wireless network connecting the first party and the second ~~party,~~<u>party and transmitting the first view of the agreement from the first party to the second party;</u> and

a wired or wireless network connecting the second party to the third ~~party;~~<u>party and transmitting the first and second views of the agreement to the third party,</u>

wherein the trusted third party~~, receiving the first view of the agreement and the second view of the agreement,~~ ~~verifying~~ <u>verifies</u> conditions <u>of the agreement</u> including ~~that the~~ identities of the <u>first and second</u> parties ~~that transmitted the agreements and that~~ <u>in</u> the independent secured <u>first and second</u> views of the agreement ~~are consistent with each other,~~ <u>based upon a symmetric agreement verification protocol using the first and second mobile device parameters for the secured first view, and</u> takes action ~~to execute~~<u>executing</u> the agreement <u>according to the verification of</u>~~if~~ the conditions <u>of the agreement</u> ~~are satisfied.~~

2.   (CURRENTLY AMENDED) A system as in ~~Claim 1~~<u>claim 1,</u> wherein the agreement pertains to ~~the~~ ordering ~~and or~~<u>and/or</u> purchasing ~~of~~ goods and<u>/or</u> services, <u>and</u> the first party <u>mobile device</u> is <u>operated by</u> a consumer, the second party is a merchant <u>device operated by a merchant,</u> and the third party is a Secure Transaction Server ~~entity.~~

3.   (CANCELLED)

4.   (CANCELLED)

5.   (CANCELLED)

6.   (CURRENTLY AMENDED) A ~~The~~ system ~~as Claim 4, where the consumer is connected to the merchant via~~according to claim 1, wherein the open and non-secure wireless network is a wireless local area network.

7.   (CANCELLED)

8.   (CURRENTLY AMENDED) The system as in ~~claim 7~~claim 2 wherein:
the ~~mobile device stores no~~input second mobile device parameter is personal identifying information about the consumer as consumer identifying information and not stored in the consumer mobile device,~~or account information of the consumer~~ and
~~such account information of the merchant and the consumer is stored in~~the trusted secure transaction server stores or ~~is accessible by the secure transaction server~~accesses the consumer identifying information.

9.   (CURRENTLY AMENDED) The system as in claim 8, further comprising one or more payment services ~~which execute~~executing a payment upon direction of the trusted secure transaction server, and
wherein the trusted secure transaction server is in secure communication with the one or more payment services, including online payment services, financial institutions, and credit card agencies, using a wired or wireless network and the trusted secure transaction server directs that payment be executed by the payment services upon ~~validation~~verification of the purchase transaction by the trusted secure transaction server.

10.   (CURRENTLY AMENDED) The system as in claim 9,
wherein the second secured view of the agreement is secured based upon both a first merchant device parameter and a second merchant device parameter input to the mobile device as merchant identifying information, and the trusted third party server verifies conditions of the agreement including identities of the first and second parties in the independent secured first and second views of the agreement, based upon a symmetric agreement verification protocol

using the first and second mobile device parameters for the secured first view and the first and second merchant device parameters for the secured second view, and

wherein the consumer identifying information and the merchant identifying information is stored only in the trusted secure transaction server, and, for authorization by the trusted secure transaction server, the merchant ~~enters~~inputs the merchant identifying information into the merchant device and the consumer ~~enters~~inputs the consumer identifying information into the consumer mobile device.

11.   (CURRENTLY AMENDED) The system as in claim 10, wherein ~~the purchase transaction is for goods and services and~~ the trusted secure transaction server supplies a token as confirmation of the payment.

12.   (CURRENTLY AMENDED) The system as in claim 11, wherein the merchant device processes the ~~consumer presents the~~ token presented by the consumer ~~to the merchant in order~~ to consume a~~the~~ good and/or service.

13.   (CURRENTLY AMENDED) The system as in ~~claim 12~~claim 2, wherein only the trusted secure transaction server, and neither the merchant device nor the consumer mobile device are able to observe details of ~~the~~ other's transaction ~~or~~including identity information of the consumer and the merchant.

14.   (CURRENTLY AMENDED) The system as in ~~claim 13~~claim 8, wherein the ~~consumer may be required to authenticate himself to the consumer device, prior to using the device, by entering~~consumer identifying information comprises one or more of a personal ~~identifying information, including but not limited to a PIN~~identification number (PIN), password, ~~or by providing~~ biometric ~~authentication, including, but not limited to~~information, a fingerprint or a voiceprint.

15.   (CURRENTLY AMENDED) The system as in claim 14, wherein the consumer only authorizes payment through an explicit command to ~~their device, by entering a personal~~the consumer mobile device by inputting the consumer identifying information~~, including but not limited to a PIN, password, or by providing biometric authentication, including, a fingerprint or a voiceprint~~.

16.   (CURRENTLY AMENDED) The system as in claim ~~15~~9, wherein ~~the consumer can select from among financial accounts of the consumer from information stored at~~ the trusted

secure transaction server ~~or accessible by the secure transaction server~~registers financial account information of the consumer for the payment services, ~~in order to use the selected account for payment~~and the consumer mobile device presents selectable financial account information of the consumer from the consumer financial account information registered by the secure transaction server.

17.   (CURRENTLY AMENDED) The system as in claim ~~16~~10, wherein the secure transaction server registers the consumer and the merchant ~~execute a registration process with the trusted third party by securely providing~~by registering financial account information of the consumer and the merchant, providing the consumer and merchant identifying information, ~~to the trusted secure transaction server~~ and ~~obtaining~~providing to the consumer mobile device and the merchant device software ~~to execute~~executing the symmetric agreement verification protocol~~Secure Transaction Protocol, and said registration procedure occurring prior to executing a purchasing transaction and said registration procedure includes providing account information and a unique identifier of the respective consumer operated device or merchant operated device and receive from the trusted secure transaction server device a personal identifying information, such as a PIN, to be only used with the respective consumer operated device or merchant operated device.~~

18.   (CURRENTLY AMENDED) A~~The~~ system as in claim 17 wherein ~~the conducting of purchase agreements, comprises:~~
~~discovering~~the consumer mobile device discovers the merchant device ~~by the consumer operating the mobile device;~~
~~selecting, by the consumer,~~the consumer mobile device receives consumer selectable goods ~~and~~/or services ~~to~~for conducting the purchase from the merchant device;
the consumer mobile device obtains~~obtaining,~~ from the merchant device, a purchase order;
the consumer mobile device receives payment authorization from ~~authorizing, by~~the consumer~~, the payment~~ for the purchase order, as the first view of the agreement ~~through the consumer device;~~
the merchant device receives authorization for acceptance of the consumer payment from the merchant, as the second view of the agreement~~authorizing, by the merchant through the merchant device, acceptance of the payment;~~
~~verifying by a trusted~~the secure transaction server verifies the conditions of the agreement~~, identities of the merchant and the consumer and details of the transaction;~~
~~causing, by the trusted~~the secure transaction ~~server,~~server as the action executing the

agreement causes payment from the consumer to the merchant through ~~a~~one of the payment ~~service~~services; and

~~issuing, by the trusted~~the secure transaction server, ~~receipts~~ issues receipts to the consumer device and to the merchant device indicating success or failure of the transaction.

19.   (CURRENTLY AMENDED) A~~The~~ system of claim 18, wherein the ~~operator of the trusted~~ secure transaction server ~~collecting~~collects a fee for processing ~~a transaction~~the purchase from one or more of the consumer, merchant, ~~or~~ payment services~~, credit card issuers and financial accounts~~ based on a fee for each ~~transaction~~purchase or on a percentage of ~~transaction~~purchase amount.

20.   (CURRENTLY AMENDED) The system as in claim 18, ~~further comprising a secure network coupling~~wherein the wired or wireless network connecting the merchant ~~operated~~ device with the ~~trusted~~ secure transaction server is a secure network and wherein the open and non-secure wireless network is a wireless local area network ~~is~~ operated by the merchant ~~operated~~ device.

21.   (CURRENTLY AMENDED) The system as in claim ~~18, further comprising a secure network coupling the merchant operated device with the trusted secure transaction server and~~20 wherein the wireless local area network includes a hotspot accessible by a plurality of ~~merchants and consumers~~merchant devices and consumer mobile devices and ~~at which~~ the consumer mobile device provides selectable ~~can select and access the merchant~~merchants based upon the merchant devices through the wireless local area network.

22.   (CANCELLED)

23.   (CURRENTLY AMENDED) The system as in claim ~~18~~20, wherein the wireless local area network includes a hotspot accessible by a plurality of ~~merchants and consumers~~merchant devices and consumer mobile devices, and ~~at which the consumer can select and access the merchant~~the consumer mobile device provides selectable merchants based upon the merchant devices through the wireless local area network, and ~~wherein~~ the merchant ~~device~~devices, the consumer ~~device~~devices, and the ~~trusted~~ secure transaction server are in communication with each other via the hotspot.

24.   (CURRENTLY AMENDED) The system as in ~~claim 18~~claim 20, wherein the merchant device executing a retail application and a secure transaction purchasing application,

can execute the secure transaction application on a local device at the merchant location connected to the wireless local area network and a remote device connected via another network to the wireless local area network and the consumer device.

25. (CURRENTLY AMENDED) The system as in any one of claims 19, 20, 21, ~~22,~~ 23, and 24, wherein the merchant device is connected to the ~~trusted~~ secure transaction server via ~~the~~ Internet using ~~additional~~ security including ~~but not limited to the~~ a secure socket layer (SSL) or a Virtual Private Network.

26. (CURRENTLY AMENDED) The system as in any one of claims 19, 20, 21, ~~22,~~ 23, and 24, wherein the ~~trusted~~ secure transaction server is connected to one or more of the payment services through a secure network or through ~~the~~ Internet using ~~additional~~ security including ~~but not limited to the~~ secure socket layer (SSL) or a Virtual Private Network.

27. (CURRENTLY AMENDED) The system as in claim 18 ~~where a consumer can request that~~ wherein the consumer mobile devices requests the Secure Transaction Server ~~disable the device and thereby not permitting further transactions~~ to disable the consumer mobile device for a purchase ~~for that device with the~~ using a current consumer identifying information ~~personal identification information~~.

28. (CURRENTLY AMENDED) The system as in claim 18 where the Secure Transaction Server ~~can detect and disable~~ detects and disables a consumer account if there are multiple attempts to authorize a payment with incorrect ~~personal~~ consumer identifying information.

29. (CURRENTLY AMENDED) The system as in claim 18, wherein ~~the consumer can purchase a service, including~~ one of the services for the purchase is a movie ticket, from the merchant ~~using a mobile~~ device; ~~receive~~ and wherein the receipt is an electronic token as proof of ~~the~~ payment; and wherein the consumer mobile device provides ~~the consumer can present~~ the token to obtain the service ~~using their mobile device~~, including a paperless e-ticket.

30. (CURRENTLY AMENDED) The system as in claim 18 where the purchase ~~transaction~~ is a return of goods and/or services from the consumer to the merchant and the secure transaction server ~~will cause~~ causes payment from the merchant to the consumer.

31. (CURRENTLY AMENDED) The system as in claim 18 in which the Secure

Transaction Server provides ancillary information from the payment services, including ~~but not limited to,~~ advertisements, special interest rate for a particular purchase if a specific credit account is chosen for ~~the~~an attempted purchase, to the consumer <u>mobile device</u> in ~~the~~ response messages prior to the ~~final purchasing~~<u>consumer payment</u> authorization ~~by the consumer~~.